

# RECEIVER APPARATUS FOR MPEG-4 IPMP EXTENDED ISMA MEDIA STREAM (4)

Patent number: JP2004364273  
 Publication date: 2004-12-24  
 Inventor: JI MING; LIU JING; SHEN MEI SHEN; UENO TAKAFUMI  
 Applicant: MATSUSHITA ELECTRIC IND CO LTD  
 Classification:  
 - international: **G06F12/14; H04L9/36; H04N7/08; H04N7/081; H04N7/16; G06F12/14; H04L9/36; H04N7/08; H04N7/081; H04N7/16; (IPC1-7): H04N7/16; G06F12/14; H04L9/36; H04N7/08; H04N7/081**  
 - european:  
 Application number: JP20040138438 20040507  
 Priority number(s): JP20040138438 20040507; JP20030131856 20030509

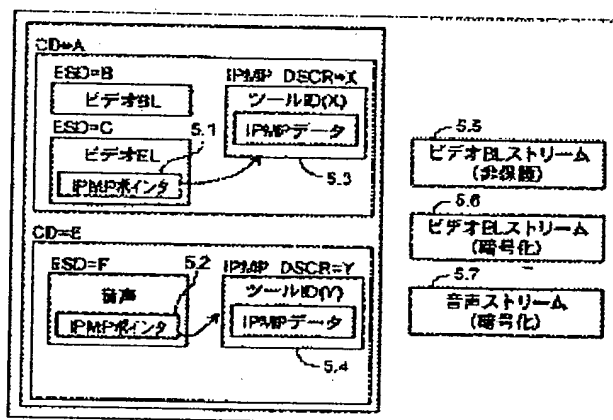
Report a data error here

## Abstract of JP2004364273

**PROBLEM TO BE SOLVED:** To provide an ISMA protection framework capable of being compatible with the MPEG-4IPMP extended standard.

**SOLUTION:** An apparatus for receiving an MPEG-4 IPMP extended ISMA media stream receives an ISMA media stream including an ISMA head, contents and an IPMP tool list descriptor indicative of a method for processing the contents, acquires the IPMP tool list descriptor from the ISMA media stream, tests whether any tool indicated by the IPMP tool list descriptor is present in the receiving apparatus, uses such tool, if present, to process the contents, and otherwise ends without failure.

COPYRIGHT: (C)2005,JPO&NCIP



Data supplied from the [esp@cenet](mailto:esp@cenet) database - Worldwide

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開2004-364273

(P2004-364273A)

(43)公開日 平成16年12月24日(2004.12.24)

(51)Int. Cl.<sup>7</sup>

F I

テーマコード (参考)

H 0 4 N 7/16

H 0 4 N 7/16

A

5 B 0 1 7

G 0 6 F 12/14

G 0 6 F 12/14

5 4 0

A

5 C 0 6 3

H 0 4 L 9/36

H 0 4 N 7/08

Z

5 C 0 6 4

H 0 4 N 7/08

H 0 4 L 9/00

6 8 5

5 J 1 0 4

H 0 4 N 7/081

審査請求 未請求 請求項の数 9

O L

(全 1 8 頁)

(21)出願番号 特願2004-138438(P2004-138438)

(22)出願日 平成16年5月7日(2004.5.7)

(31)優先権主張番号 特願2003-131856(P2003-131856)

(32)優先日 平成15年5月9日(2003.5.9)

(33)優先権主張国 日本国(JP)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(74)代理人 100086405

弁理士 河宮 治

(74)代理人 100098280

弁理士 石野 正弘

(74)代理人 100113170

弁理士 稲葉 和久

(72)発明者 ジ・ミン

シンガポール534415シンガポール、タイ・

セン・アベニュー、ブロック1022、06-3

530番、タイ・セン・インダストリアル・

エステイト、パナソニック・シンガポール

研究所株式会社内

最終頁に続く

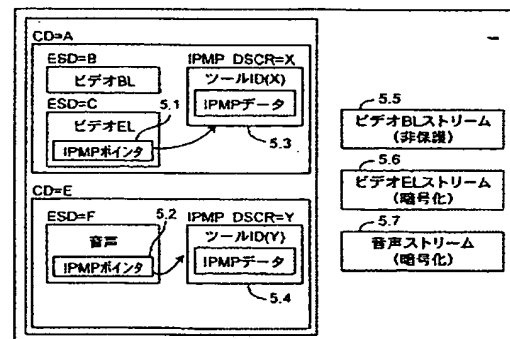
(54)【発明の名称】MPEG-4 IPMP拡張されたISMA媒体ストリームの受信装置

(57)【要約】

【課題】 ISMA保護フレームワークについて互換可能なMPEG-4 IPMP拡張を提供する。

【解決手段】 MPEG-4 IPMP拡張されたISMA媒体ストリームを受信する装置であって、ISMAヘッドと、コンテンツと、前記コンテンツの処理方法を示すIPMPツールリスト記述子とを含むISMA媒体ストリームを受信し、前記ISMA媒体ストリームから前記IPMPツールリスト記述子を取得し、前記IPMPツールリスト記述子に示されたツールが前記受信装置に存在するか否か进行检查し、前記ツールが存在する場合には前記ツールを用いて前記コンテンツを処理し、前記ツールがない場合には破綻することなく終了する。

【選択図】 図5



**【特許請求の範囲】****【請求項 1】**

MPEG-4 IPMP拡張された ISMA媒体ストリームを受信する装置であって、  
ISMAヘッドと、コンテンツと、前記コンテンツの処理方法を示す IPMPツールリス  
ト記述子とを含む ISMA媒体ストリームを受信し、

前記 ISMA媒体ストリームから前記 IPMPツールリスト記述子を取得し、

前記 IPMPツールリスト記述子に示されたツールが前記受信装置に存在するか否かを  
検査し、

前記ツールが存在する場合には前記ツールを用いて前記コンテンツを処理し、前記ツ  
ールがない場合には破綻することなく終了する受信装置。

10

**【請求項 2】**

前記 ISMA媒体ストリームは IODを有し、前記 IPMPツールリスト記述子を前記  
IODから取得することを特徴とする請求項 1に記載の受信装置。

**【請求項 3】**

MPEG-4 IPMP拡張された ISMA媒体ストリームを受信する装置であって、  
ISMAヘッドと、コンテンツと、前記コンテンツの処理方法を示す IPMP記述子と  
を含む ISMA媒体ストリームを受信し、

前記 ISMA媒体ストリームから前記 IPMP記述子を取得し、

前記 IPMP記述子に示されたツールが前記受信装置に存在するか否かを検査し、

前記ツールが存在する場合には前記ツールを用いて前記コンテンツを処理し、前記ツ  
ールがない場合には破綻することなく終了する受信装置。

20

**【請求項 4】**

前記 ISMA媒体ストリームはさらに、前記 IPMP記述子を指す IPMP記述子ポイ  
ンタを含み、前記受信装置は前記 ISMA媒体ストリームから、前記 IPMP記述子ポイ  
ンタを取得して、

前記 IPMP記述子ポインタが指すアドレスの前記 IPMP記述子を取得することを特  
徴とする請求項 3に記載の受信装置。

**【請求項 5】**

前記 IPMP記述子ポインタを前記 ISMA媒体ストリームの ES記述子から取得し、  
前記 IPMP記述子ポインタが指す前記 IPMP記述子を前記 ISMA媒体ストリームの  
ODから取得することを特徴とする請求項 4に記載の受信装置。

30

**【請求項 6】**

前記 IPMP記述子で ISMACryp解読ツールが指定されている場合、前記 ISM  
ACryp解読ツールを起動して、前記コンテンツの解読を行うことを特徴とする請求項  
3から 5のいずれか一項に記載の受信装置。

**【請求項 7】**

前記 IPMP記述子に格納されている ISMACryp\_Dataから ISMACryp  
pパラメータを取り出し、

前記取り出された ISMACrypパラメータを用いて ISMACryp解読ツールを  
設定して、前記コンテンツの解読を行うことを特徴とする請求項 6に記載の受信装置。

40

**【請求項 8】**

前記 ISMA媒体ストリームの IPMPストリーム内の IPMPメッセージに格納され  
ている ISMACryp\_Dataから ISMACrypパラメータを取り出し、

前記取り出された ISMACrypパラメータを用いて ISMACryp解読ツールを  
設定し、前記コンテンツの解読を行うことを特徴とする請求項 6に記載の受信装置。

**【請求項 9】**

前記 ISMA媒体ストリームは、前記 IPMP記述子に加えて、さらに前記少なくとも  
一つのツールを示す IPMPツールリスト記述子を含み、

前記受信装置は、前記 IPMPツールリスト記述子又は前記 IPMP記述子を取得して  
、前記 IPMPツールリスト記述子又は前記 IPMP記述子に示されたツールが前記受信

50

装置に存在するか否かを検査することを特徴とする請求項3に記載の受信装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ISMA保護フレームワークについて互換可能なMPEG-4 IPMP拡張に関する。

【背景技術】

【0002】

この数年間、媒体コンテンツ流通業界ではインターネットを介したビデオや音声の配信を保証することが広く推進されてきた。各種の標準化団体がこの問題に対する解決策を提供すべく多大な努力をしてきた。インターネット・ストリーミングメディア・アライアンス (ISMA: Internet Streaming Media Alliance) はこのような団体の一つである。

IPフレームワークおよびインターネットで利用できるビデオや音声システムをベンダーが構築するために使用可能な、既存のオープンスタンダードを使用したフレームワークを明示することにより、このニーズに応えようとするものである。その仕様は既存のMPEG技術を使用することを想定しており、主に現段階のMPEG-4技術に焦点を合わせているが、将来的にはMPEG-2およびMPEG-7技術を含む変更や修正を予定している。

【0003】

ISMAはまた、ISMA媒体ストリーム用に暗号化フレームワーク、すなわちISMACrypも規定している。このフレームワークは新規の媒体符号化に拡張可能であり、新規の暗号化へ対応可能であって、しかも各種の暗号鍵管理、セキュリティ、あるいはデジタル権利管理 (DRM) システムに適用可能である。これはまた、ISMA仕様向けの媒体ストリームおよび媒体メッセージの認証用のデフォルト暗号方式も規定する。図1に、ISMAフレームワーク用のISMACryp保護のアーキテクチャ図を示す。図1のISMA DRMの範囲は、ISMA媒体の暗号化及びISMAメッセージの認証であり、図では"ISMACryp"とラベルされており、ISMACrypのシグナリングは"RTSP/SDP+" (ISMA1.0 SDPディフィニション・プラスISMACrypシグナリング) とラベルされている。マスタリング (1.1) は、コンテンツの準備及び発行を担っている。鍵/ライセンス管理インタフェースのためのプロトコルはISMACrypの範囲外である。また、図1において、鍵/ライセンス管理からISMA受信機への鍵 (又はライセンス) の配送は、ISMACrypの範囲外である。ISMACryp技術開発の目的は、上記のような情報を端末まで配送する安全な方法にあると考えられる。送信機 (1.2) は、RTSP/SDP+ (ISMA1.0 SDPディフィニション・プラスISMACrypシグナリング) を用いてISMA送信機でシグナリングされるか、又は第3デバイスによってシグナリングされる"ISMACryp"と呼ばれるオープンスタンダードなプロトコルを介してISMA受信機への配送を担う。

【0004】

ISMA DRMアーキテクチャでは、ISMA受信機はISMACryp暗号化されたストリーム、認証されたメッセージ、及びシグナリングを処理できる。"ISMACryp"は、ISMA1.0 媒体及び暗号化、メッセージ認証、全体サービスを備えたプロトコルを提供する技術である。

【0005】

図2は、鍵/ライセンス管理 (KEY MGT)、RTSP制御インタフェース、及びISMAデータ用の暗号化サービスであるISMACrypへのインタフェースを伴うISMA受信機アーキテクチャを示すさらに詳細な図である。ISMACryp受信機は、ISMAデータを暗号化し、認証し、その完全性をチェックできる。

【0006】

図3は、ストリームがファイルにマスタリングされ、又はエンコーディングからネットワークに直接にストリーミングされるISMACryp環境を示す図である。いずれの場合

合にも、配送の前に暗号化されるが、メッセージ認証は配送時に行われる。受信機（媒体再生機／デコーダ）では、ストリームはプレーヤ、キャッシュサーバでのパーソナルレコーダ等のファイルに受信されるか、又は直接デコーダに受信される。ISMACryp変換はエンコーダ／送信機で行われ、解読はデコーダ／受信機で終端するアーク（arc）上で行われる。

#### 【0007】

ISMAの宣言に従い、2種類の受信機、すなわちISMA専用受信機およびMPEGシステム対応受信機を対象とする。ここで“ISMA専用受信機”とはMPEG-4システム対応でない、すなわちMPEG-4信号通知（シグナリング）およびMPEG-4（基本）媒体ストリームを伴う制御（基本）ストリームを一切処理することができない受信機と定義する。これに対し、“MPEGシステム対応受信機”はISMA関連情報だけでなく、MPEG-4システムレイヤ情報を処理することができる。MPEGシステム対応受信機との相互運用可能性は、少なくとも最小限のMPEGシステムシグナリングを搬送するMPEG IOD（初期オブジェクト記述）を介して実現される。IODはバイナリSDP（セッション記述プロトコル）属性、すなわちSDP IODとして含まれる。

#### 【0008】

ISMACrypはまた、両方のタイプの受信機に適用できる。SDPメッセージ内のバイナリIODを拡張する。新規のシグナリングはISMAシグナリングに見られる冗長性よりもむしろ非対称に主眼を置く。SDP IODの“最小”および“基本”シグナリングパラメータを提供して、受信機のMPEG-4 IPMPシステムとの相互運用性を最大にする。

#### 【0009】

しかし、現行のISMACryp規定によるIODの拡張は完全ではなく、最新のMPEG-4 IPMP拡張標準との整合性がない。この結果、ISMAストリームはMPEG-4 IPMP拡張互換受信機により正しく認識されない恐れがある。例えば、ISMACryp標準はIOD内におけるIPMP\_Descriptorの存在を使用してISMACryp保護をシグナリングすると規定している。しかし、MPEG-4 IPMP拡張によれば、IPMP保護が存在する場合はIOD内にツールリスト記述子を提示すべきである。これらの不完全性や不整合性はISMAフレームワークのMPEG-4 IPMP拡張互換受信機との相互運用可能性を阻害しかねない。

#### 【発明の開示】

#### 【発明が解決しようとする課題】

#### 【0010】

本発明は以下の課題を解決しようとするものである。

ISMACryp標準はSDP内のIOD拡張を介してMPEG-4 IPMPを用いることにより、ISMACryp保護のシグナリングを規定する。IOD内におけるIPMP\_Descriptorの存在は受信機に対し、この媒体ストリームが保護されていること通知する。MPEG IPMP非互換受信機の場合、独自ながら適切な方法でストリームを処理することが許される。例えば、単にストリームを無視する。しかし、MPEG-4 IPMP拡張標準は、IOD内にツールリスト記述子を提示してIPMP保護を示すべきであると規定している。標準では、IPMP保護のためにIODにIPMP\_Descriptorが存在することを保証していない。従って、ISMACrypで規定されたシグナリング方法では、IODがツールリスト記述子を含むがIPMP\_Descriptorは含んでいない媒体ストリームが保護されている仕組みを正確に検知できない恐れがある。

#### 【0011】

さらに、MPEG-4 IPMP拡張互換受信機がISMA関連データ、例えばIPMPデータに伴う暗号化情報やKMS構成を受信可能にするために、ISMACryp標準はMPEG-4 IPMP標準に基づいて自己規定されたISMACryp\_DescriptorによりIOD内のIPMP\_Descriptorを拡張する。しかし、MP

10

20

30

40

50

EG-4 IPMP標準の改訂が速いために、IODのシンタックスは変更されていて、ISMACryp標準に基づく旧バージョンとは異なる。このことは、IPMPコンテキストに格納されたISMA関連データを最新のMPEG-4 IPMP拡張標準と互換性のある受信機を識別できない恐れがあるという問題をもたらす。既に規定済みのISMAパラメータの変更を最小にとどめながら、最新のMPEG-4 IPMP拡張標準の一貫性を保つために、現行MPEG-4 IPMP拡張標準によりISMA関連のデータを格納することが可能な新しい仕組みが必要とされており、その仕組みはMPEG-4 IPMP拡張標準の旧バージョンとは後方互換性（バックワードコンパチブル）が求められる。

【0012】

本発明は、ISMA保護フレームワークについて互換可能なMPEG-4 IPMP拡張を提供することを目的とする。

【課題を解決するための手段】

【0013】

本発明はシグナリング問題を扱うために、MPEG初期オブジェクト記述子（IOD）におけるISMACryp保護の存在をシグナリングするシグナリング機構を規定する。ツールリストおよびIPMP記述子を使用して保護をシグナリングする。この手段は最新のMPEG-4 IPMP拡張標準と互換性があり、同時にMPEGシステム対応ISMA受信機との互換性を最大限に提供する。また、コンテンツを再生するよう要求されたツールを識別するための柔軟な方法を提供する。

【0014】

本発明はまた、ISMACrypパラメータを格納してMPEGシステム対応ISMA受信機用に変換する仕組みを規定する。MPEG-4 IPMP拡張により規定されたIPMP\_Data\_BaseClassからISMA専用Cryp\_Dataを拡張してISMACrypパラメータを格納することができる。このISMACryp\_Dataは次いでMPEG-4 IPMP拡張標準に準拠するためにIPMP記述子またはIPMPストリームに格納することができる。

【0015】

本発明に係るMPEG-4 IPMP拡張されたISMA媒体ストリームを受信する装置では、

ISMAヘッドと、コンテンツと、前記コンテンツの処理方法を示すIPMPツールリスト記述子とを含むISMA媒体ストリームを受信し、

前記ISMA媒体ストリームから前記IPMPツールリスト記述子を取得し、

前記IPMPツールリスト記述子に示されたツールが前記受信装置に存在するか否かを検査し、

前記ツールが存在する場合には前記ツールを用いて前記コンテンツを処理し、前記ツールがない場合には破綻することなく終了する。

【0016】

なお、破綻することなく終了するとは、あらかじめ定められた処理を行って終了することをいう。破綻とは、例えば、ハングアップ等を意味する。

【0017】

また、前記ISMA媒体ストリームはIODを有し、前記IPMPツールリスト記述子を前記IODから取得する。

【0018】

さらに、本発明に係るMPEG-4 IPMP拡張されたISMA媒体ストリームを受信する装置では、

ISMAヘッドと、コンテンツと、前記コンテンツの処理方法を示すIPMP記述子とを含むISMA媒体ストリームを受信し、

前記ISMA媒体ストリームから前記IPMP記述子を取得し、

前記IPMP記述子に示されたツールが前記受信装置に存在するか否かを検査し、

前記ツールが存在する場合には前記ツールを用いて前記コンテンツを処理し、前記ツールがない場合には破綻することなく終了する。

【0019】

また、前記 ISMA 媒体ストリームはさらに、前記 IPMP 記述子を指す IPMP 記述子ポインタを含み、前記受信装置は前記 ISMA 媒体ストリームから、前記 IPMP 記述子ポインタを取得して、

前記 IPMP 記述子ポインタが指すアドレスの前記 IPMP 記述子を取得することが好ましい。

【0020】

なお、前記 IPMP 記述子ポインタを前記 ISMA 媒体ストリームの ES 記述子から取得し、前記 IPMP 記述子ポインタが指す前記 IPMP 記述子を前記 ISMA 媒体ストリームの OD から取得する構成としてもよい。 10

【0021】

また、前記 IPMP 記述子で ISMACryp 解読ツールが指定されている場合、前記 ISMACryp 解読ツールを起動して、前記コンテンツの解読を行うこととしてもよい。

【0022】

さらに、前記 IPMP 記述子に格納されている ISMACryp\_Data から ISMACryp パラメータを取り出し、

前記取り出された ISMACryp パラメータを用いて ISMACryp 解読ツールを設定して、前記コンテンツの解読を行う構成としてもよい。 20

【0023】

またさらに、前記 ISMA 媒体ストリームの IPMP ストリーム内の IPMP メッセージに格納されている ISMACryp\_Data から ISMACryp パラメータを取り出し、

前記取り出された ISMACryp パラメータを用いて ISMACryp 解読ツールを設定し、前記コンテンツの解読を行う構成としてもよい。

【0024】

また、前記 ISMA 媒体ストリームは、前記 IPMP 記述子に加えて、さらに前記少なくとも一つのツールを示す IPMP ツールリスト記述子を含み、 30

前記受信装置は、前記 IPMP ツールリスト記述子又は前記 IPMP 記述子を取得して、前記 IPMP ツールリスト記述子又は前記 IPMP 記述子に示されたツールが前記受信装置に存在するか否かを検査する構成としてもよい。

【0025】

ところで、ISMA フレームワーク内では IOD および OD が構成される。IPMP ツールリスト記述子は IOD 内に埋め込まれ、ISMACryp 保護が存在する場合は、IPMP 記述子ポインタおよび IPMP 記述子が IOD および OD 内に埋め込まれる。

【0026】

IOD および OD は、SDP IOD シグナリングを介して MPEG-4 システムを理解する ISMA 受信機へ搬送される。受信機は IOD と OD を解析する。IPMP ツールリストを検知したならば、受信機は ISMACryp 保護が存在することを認識している。IPMP 記述子ポインタと IPMP 記述子を検知したならば、受信機はどのストリームがどのツールで保護されているかを認識できる。 40

【0027】

ISMA フレームワーク内において、ストリームが ISMAMACryp により保護されている場合、ISMACryp パラメータ（例えば暗号識別子）は ISMACryp\_Data に格納されて、IPMP 記述子または IPMP ストリームに入れることができ、パラメータの格納は MPEG-4 IPMP 拡張に準拠している。

【0028】

受信機側で、ISMACryp 用のパラメータを、MPEG-4 IPMP 拡張と互換 50

性を保ちつつIPMP記述子またはISMACrypストリームから取出すことができる。次いでこのパラメータを用いてISMACryp解読ツールを設定することができる。

#### 【0029】

本発明を使用することにより、ISMA保護フレームワークはMPEG-4 IPMP拡張互換受信機との相互運用を可能にする。

#### 【0030】

本発明はIOD内のツールリスト、およびOD内のIPMP記述子を用いてISMACryp保護をシグナリングする。それにより、シグナリング方法は柔軟にでき、最新のMPEG-4 IPMP拡張標準と真に互換性を有し、従ってMPEGシステム対応ISMA受信機を相互運用可能にする。

#### 【0031】

本発明はまた、IPMP\_Data\_BaseClassから拡張したISMACryp\_Dataを生成する。本発明によるISMACryp\_Dataを用いて、ISMACrypパラメータを格納し、続いてIPMP記述子またはIPMPストリームのいずれかに格納することができる。ISMACrypパラメータの格納は今やMPEG-4 IPMP拡張遵守事項になっている。

#### 【発明を実施するための最良の形態】

#### 【0032】

##### IPMP拡張シグナリング

現行ISMACrypはISMA専用およびMPEG受信機向けのSDP IODシグナリングに対応している。ISMA専用受信機はSDP FMTPシグナリングパラメータのみ受理するが、SDP IODはストリームがISMACryp保護（最小IPMPシグナリング）されて任意のMPEG受信機にシグナリングしなければならない。KMSは、SDP IOD内のIPMPシグナリング（基本IPMPシグナリング）のみを用いてISMACrypをシグナリングしてもよい。

#### 【0033】

本明細書ではMPEG-4 IPMP拡張と互換性を有するシンタックスを提供する。最小限の労力で、ISMACrypは容易にMPEG-4 IPMP拡張との互換性を実現することができ、さらに柔軟な保護スキームを提供する。

#### 【0034】

##### 最小IPMP-Xシグナリング

IPMP拡張はIODにおけるIPMPツールリスト記述子を規定する。ツールリスト記述子は後で出てくるストリーム列で必要とされるIPMPツールのリストを識別する。MPEG-4 IPMP拡張によれば、IPMP保護が存在する場合、ツールリスト記述子はIOD内に提示されるべきである。従って、最小限のIPMP-Xシグナリングの場合、この目的を実現するにはIPMP記述子の代わりにIOD内のIPMPツールリスト記述子を使用することを提案する。

#### 【0035】

SDPによりMPEG-4 IODに持ち込まれたIODにおけるIPMPツールリストの位置は、図6で6.1として示されている。

#### 【0036】

暗号化およびKMS情報移送を指定する現行のISMACryp仕様によれば、少なくとも2個のツールがMPEG IPMPツールリスト記述子に提示されるべきである。最初のものはKMSツールであり、他のものはISMA解読ツールである。MPEG IPMPツールリストにおけるISMACrypツールの存在はISMACryp保護をシグナリングする。

#### 【0037】

ISMACrypツールを有するツールリスト記述子の例を表1に示す。

10

20

30

40



【表 1】

IPMP_ToolListDescriptor			
1	8	IPMP_ToolListDescTag	0×60
2	16	記述子のサイズ	
IPMP_Tool			
3	8	IPMP_ToolTag	0×61
4	16	記述子のサイズ	
5	128	IPMP_ToolID	値は各サービスプロバイダが自身のKMS ツールへ割当
6	1	isAltGroup	0
7	1	isParametric	0
8	6	予約	0b0000.00
9	8	ツールURLのサイズ	
10		ツールURL	
IPMP_Tool			
11	8	IPMP_ToolTag	0×61
12	16	記述子のサイズ	
13	128	IPMP_ToolID	値はISMA解読ツールへ割当
14	1	isAltGroup	0
15	1	isParametric	0
16	6	予約	0b0000.00
17	8	ツールURLのサイズ	
18		ツールURL	

## 【0038】

IPMPツールリストは図4に示すMPEG-4 IPMP拡張コンテンツ構造で示される。IPMPツールリスト(4.1)を用いることにより、ISMACryp保護の存在のシグナリングを容易にするだけでなく、ツールの識別を極めて柔軟に行なえるようにする。ツールリストでのIPMPツールは3通りの方法で識別可能である。第一は値が公的登録機関により割り当てられた固定128ビットIPMP\_\_ToolID(4.2)を使用する。第二は相互に同等な代替物であるツールを示すIPMP\_\_ToolID(4.3)のリストを使用する。そうすることにより、端末はより柔軟に自身のツール選択を行なうことができる。最後のものはIPMPツールが満たすべき基準を記述するためのパラメータ表記(4.4)を使用するが、この場合、端末は必要な機能を実行するためのツール選択の自由度が大きくなる。

## 【0039】

## 基本IPMP-Xシグナリング

MPEGシステム対応受信機の場合、IPMP関連の処理のためにより多くのIPMP情報が必要とされる。より高性能なMPEG IPMP拡張シグナリングのベースとして以下のIPMP-Xシグナリングを使用する。セクション2で紹介したツールリストと共に、MPEG互換受信機が必要とするベース情報を提供する。暗号化された基本ストリームに対し、対応するES記述子は以下のIPMP\_DescriptorPointer(表2)を含んでいなければならない。

## 【0040】

10

20

30

40

50

【表 2】

記述子名			
フィールド ド番号	ビットサ イズ	フィールド名	値
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	記述子サイズ	5
3	8	IPMP_DescriptorID	0×FF
4	16	IPMPX_DescriptorID	0×0002/0×0003
5	16	IPMP_ES_ID	0×0000

## 【0041】

このIPMP拡張保護シグナリングの概念を図5に示す。ES\_Descriptor内のこの記述子ポインタ（5. 1および5. 2）が存在することで、この記述子に関連付けられたストリームは、参照IPMP\_Descriptor（5. 3および5. 4）で指定されたIPMPツールにより保護および管理される対象であることを示す。表3に示す参照IPMP\_Descriptorは、オブジェクト記述子に格納されるべきである。

## 【0042】

SDPによってMPEG-4 IOD内に持ち込まれたODストリームにおけるIPMP記述子の位置は、図6に符号6. 2として示されている。

【表 3】

記述子名			
フィールド ド番号	ビットサ イズ	フィールド名	値
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	記述子サイズ	23
3	8	IPMP_DescriptorID	0×FF
4	16	IPMPS_Type	0×FFFF
5	16	IPMP_DescriptorIDex	0×0002/0×0003
6	128	IPMP_ToolID	値はISMA解読ツールへ割当
7	8	制御ポイントコード	0×01（解読バッファと解読器の間）
8	8	シーケンスコード	0×80

## 【0043】

また、IODは以下のIPMP\_DescriptorPointer（表4）を含んでいる必要がある。以下の例で、参照記述子で示した特定のDRMツール（暗号鍵管理システム）がグローバル・スコープでインスタンス生成される必要があることがわかる。

## 【0044】

【表 4】

記述子名			
フィールド番号	ビットサイズ	フィールド名	値
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	記述子サイズ	5
3	8	IPMP_DescriptorID	0×FF
4	16	IPMP_DescriptorIDEx	0×0001
5	16	IPMP_ES_ID	0×0000

10

## 【0045】

上のIPMP\_DescriptorPointerは、IPMP\_DescriptorIDExが0×0001であるIPMP\_Descriptorを指示する。次いで指定されたIPMP\_DescriptorがIOD（表5）に提示される必要がある。KMSの場合、記述子の制御ポイントはグローバル・スコープであることを示すために0×00に設定すべきである点に留意されたい。

20

## 【0046】

【表 5】

記述子名			
フィールド番号	ビットサイズ	フィールド名	値
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	記述子サイズ	22
3	8	IPMP_DescriptorID	0×FF
4	16	IPMPS_Type	0×FFFF
5	16	IPMP_DescriptorIDEx	0×0001
6	128	IPMP_ToolID	値は各サービスプロバイダによりKSMツールに割当
7	8	制御ポイントコード	0×00(制御ポイント無し)

30

## 【0047】

IPMP拡張と互換性のある仕方でISMACrypデータを格納

40

ISMACrypはパラメータの組を用いてストリームの暗号化を記述する。パラメータの組を以下にリストする。

## 【0048】

【表 6】

パラメータ	値	意味	デフォルト
Crypto-suite	1..255	暗号、モード、鍵長さ、等	1 <sup>1)</sup>
IV-length	1..8	IVのバイト単位の長さ	4
Delta-IV-length	0..2	デルタIVのバイト単位の長さ	0
Selective-encryption	0..1	ストリームを選択的に暗号化する場合、'1'を設定する	0
Key-indicator-per-AU	0..1	複数の鍵インジケータがパケットにおいて現れる場合、'1'を設定する	0
Key-indicator-length	0..255	鍵インジケータのバイト単位の長さ	0

1) セクション10.0のAES-CTRデフォルト

## 【0049】

IPMP拡張と互換性のある仕方でパラメータを格納するために、ISMACryp\_DataはIPMP-Xにより規定されたIPMP\_Data\_BaseClassから拡張可能である。IPMP\_Data\_BaseClassは以下に示すように、MPEG-4 IPMPXで規定される。

## 【0050】

```
abstract aligned(8) expandable(2^28-1) class IPMP_Data_BaseClass:
    bit(8) tag=0 ... 255
{
    bit(8)      Version;
    bit(32)     dataID;
    // Fields and data extending this message.
}
```

## 【0051】

ISMACryp\_Dataはユーザー定義のタグを用いて上のベースクラスから拡張可能である。次いでデータはパラメータを格納すべく自身のフィールドの組を持つことができる。これにより同じコンテンツストリームを解釈する異機種ISMA端末の互換性が保証される。

## 【0052】

このISMACryp\_Dataは標準的な仕方で2箇所に格納することができる。第一はIPMP記述子への格納である。このISMACryp\_Dataを有するIPMP記述子の例を表7に示す。

## 【0053】

10

20

30

【表 7】

記述子名			
フィールド 番号	ビットサ イズ	フィールド名	値
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	記述子サイズ	23
3	8	IPMP_DescriptorID	0×FF
4	16	IPMPS_Type	0×FFFF
5	16	IPMP_DescriptorIDEx	0×0002/0×0003
6	128	IPMP_ToolID	値は ISMA 記述子ツールへ割 当
7	8	制御ポイントコード	0×01 (解読バッファと解読器の 間)
8	8	シーケンスコード	0×80
		ISMACryp_Data	
7	8	ISMACryp_DataTag	規定予定
8	8	データサイズ	20
9	8	暗号の組	暗号記述子
11	4	IV-length	初期化ベクトルのバイト長
12	2	Delta-IV-length	AUベースのIVのバイト長
13	1	Selective-encryption	選択的暗号化を用いた場合 1
14	1	Key-indicator-per-Au	パケットに複数の鍵インジケー タが出現した場合に 1
15	8	Key-indicator-length	鍵インジケータのバイト長

## 【0054】

SDPによりMPEG-4 IOD内に持ち込まれたIPMP記述子のODストリームにおける位置は、図6で符号6. 2として示されている。

## 【0055】

ISMACryp\_Data を格納する第二の方法は、IPMP\_Message内のペイロードとして格納し、続いてMPEG-4 IPMP拡張で規定されているようにIPMPストリームに格納する。

## 【0056】

aligned(8) expandable(228-1) class IPMP\_Message

```
{
    bit(16)    IPMPS_Type;
    if (IPMPS_Type == 0)
    (
        bit(8) URLString[sizeofInstance-2];
    )
    else (if (IPMPS_Type == 0×0001)
    (
```

```

    bit(16) IPMP_DescriptorID;
    IPMP_Data_BaseClass IPMP_ExtendedData[]
} else {
    bit(8) IPMP_data[sizeofInstance-2];
}
}

```

## 【0057】

表8に、IPMP\_MessageがISMACryp\_Dataを格納している場合のシンタックスを示す。このIPMP\_DescriptorIDExを有するIPMP記述子で指定されたIPMPツールがIPMP\_Messageの宛先である。

## 【0058】

【表8】

フィールド番号	ビットサイズ	フィールド名	値
		IPMP_Message	
1	16	メッセージサイズ	
2	16	IPMPS_Type	0×0001
3	16	IPMP_DescriptorIDEx	
		ISMACryp_Data	
4	8	ISMACryp_DataTag	規定予定
5	8	データサイズ	20
6	8	暗号の組	暗号識別子
7	4	IV-length	初期化ベクトルのバイト長
8	2	Delta-IV-length	AUベースのIVのバイト長
9	1	Selective-encryption	選択的暗号化を用いた場合1
10	1	Key-indicator-per-Au	パケットに多キーインジケータ が出現した場合1
11	8	Key-indicator-length	キーインジケータのバイト長

## 【0059】

ISMA受信機でのIPMPXシグナリングの処理

上記IPMPXシグナリングに従って、ISMA受信機ではストリームが保護されているか否かを特定でき、保護されている場合には、どのように処理するか特定できる。

## 【0060】

ISMA受信機で関連付けられた媒体ストリームを記述するSDPパラメータを取得した場合(S01)、MPEG-4 IODと呼ばれる属性があるか否かをチェックし(S02)、それが存在する場合にはその関連付けられた媒体ストリームはMPEG-4システムと互換性のあるストリームであることがわかる。存在しない場合には、非MPEG方法で処理する(S03)。次に、MPEG-4 IOD内にIPMPツールリストが存在するか否かをチェックする(S04)。MPEG-4 IOD内にIPMPツールリストが存在する場合、IPMP拡張を用いてその媒体ストリームが保護されていることがわかる。そしてIPMP記述子で特定されたTool\_IDに従ってツールを立ち上げる(S06)。KMSツールを立ち上げて鍵管理問題を取り扱い、暗号解読ツールを立ち上げて特定された制御ポイントで媒体ストリームの暗号解読を取り扱う(S07)。また、IPMP記述子又はIPMPストリームに持ち込まれたISMACryp\_Dataがあるか

10

20

30

40

50

否かをチェックし（S08）、それがあある場合には、それを暗号解読ツールに配送し、設定する（S09）。なお、上記ステップS04でIPMPツールリストが存在しない場合には、IPMP保護でないMPEG方法で処理する（S05）。上記プロセスを図7に示した。

#### 【0061】

なお、本発明は、様々な実施の形態に示されている以下の構成をとることができる。第1の構成によれば、ISMA受信機側でMPEG-4 IPMP拡張を使用してISMA媒体ストリームの柔軟な保護を行なう装置であって、

IODからIPMPツールリスト記述子を受信する工程と、

ツールリストに示されたツールを検査し、ツールIDで識別されるISMACryp解読ツールがある場合、前記ISMACryp解読ツールが存在するか否かを検査し、存在しない場合、受信機は破綻することなく受信を拒否する工程と、

ツールリストに示されたツールを検査し、ツールIDで識別されるISMACrypKMSツールがある場合、ISMACrypKMSツールが存在するか否かを検査し、存在しない場合、受信機は破綻することなく受信を拒否する工程とを含む。

#### 【0062】

第2の構成によれば、上記記載のISMA受信機側でMPEG-4 IPMP拡張を使用してISMA媒体ストリームの柔軟な保護を行なう装置であって、前記IPMPツールリストを検査する工程は、

ES記述子からIPMP記述子ポインタを受信し、参照IPMP記述子をODから受信する工程と、

ISMACryp解読ツールがIPMP記述子で指定されている場合、ISMACryp解読ツールを起動し、前記ES記述子の記述に従い保護された媒体ストリームの解読を開始する工程とをさらに含む。

#### 【0063】

第3の構成によれば、上記記載のISMA受信機側でMPEG-4 IPMP拡張を使用してISMA媒体ストリームの柔軟な保護を行なう装置であって、前記IPMPツールリストを検査する工程は、

ES記述子からIPMP記述子ポインタを受信し、参照IPMP記述子をODから受信する工程と、

ISMACryp解読ツールがIPMP記述子で指定されている場合、ISMACryp解読ツールを起動する工程と、

IPMP記述子に格納されているISMACryp\_DataからISMACrypパラメータを取出す工程と、

前記取出されたISMACrypパラメータを用いてISMACryp解読ツールを設定し、前期ES記述子を参照して保護された媒体ストリームの解読を開始する工程とをさらに含む。

#### 【0064】

第4の構成によれば、上記記載のISMA受信機側でMPEG-4 IPMP拡張を使用してISMA媒体ストリームの柔軟な保護を行なう装置であって、前記IPMPツールリストを検査する工程は、

ES記述子からIPMP記述子ポインタを受信し、参照IPMP記述子をODから受信する工程と、

ISMACryp解読ツールがIPMP記述子で指定されている場合、ISMACryp解読ツールを起動する工程と、

IPMPストリーム内のIPMPメッセージに格納されているISMACryp\_DataからISMACrypパラメータを取出す工程と、

前記取出されたISMACrypパラメータを用いてISMACryp解読ツールを設

10

20

30

40

50

定し、前記ES記述子を参照して保護された媒体ストリームの解読を開始する工程とをさらに含む。

【0065】

上述の通り、本発明は好ましい実施形態により詳細に説明されているが、本発明はこれらに限定されるものではなく、以下の特許請求の範囲に記載された本発明の技術的範囲内において多くの好ましい変形例及び修正例が可能であることは当業者にとって自明なことであろう。

【図面の簡単な説明】

【0066】

【図1】 ISMACrypのアーキテクチャを示す。

10

【図2】 IPMPCryp受信機のアーキテクチャを示す図である。

【図3】 IPMPCrypを用いる保護の端末間フローを示す図である。

【図4】 MPEG-4 IPMP拡張コンテンツ構造を示す。

【図5】 IPMP記述子を用いた保護シグナリングを示す図である。

【図6】 SDP内に持ち込まれたIODにおけるIPMP情報を示す図である。

【図7】 ISMA受信機でのIPMP-X処理のフローチャートである。

【符号の説明】

【0067】

1. 1 マスタリング

1. 2 送信機

20

4. 1 IPMPツールリスト

4. 2 ツールID群

4. 3 代替ツールID群

4. 4 パラメータ記述

5. 1、5. 2 IPMPポインタ

5. 3、5. 4 IPMP記述子

5. 5 ビデオBLストリーム

5. 6 ビデオELストリーム

5. 7 音声ストリーム

6. 1 IPMPツールリスト

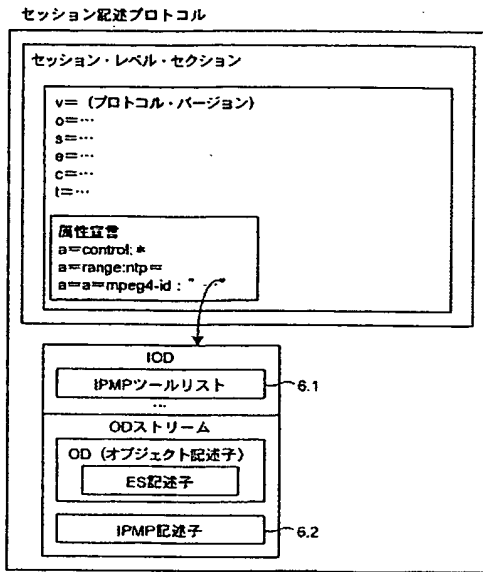
30

6. 2 IPMP記述子

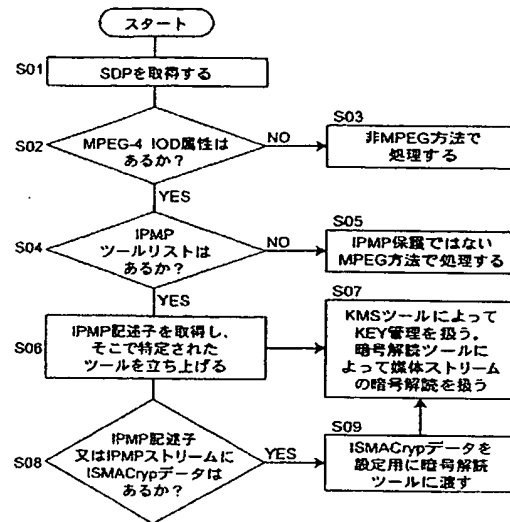




【図 6】



【図 7】



-----  
フロントページの続き

(72)発明者 リュウ・ジン

シンガポール 534415 シンガポール、タイ・セン・アベニュー、ブロック 1022、06-3  
530 番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式  
会社内

(72)発明者 シェン メイ・シェン

シンガポール 534415 シンガポール、タイ・セン・アベニュー、ブロック 1022、06-3  
530 番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式  
会社内

(72)発明者 上野 孝文

大阪府門真市大字門真 1006 番地 松下電器産業株式会社内

F ターム(参考) 5B017 AA08 BA07

5C063 AA01 AB03 AB07 AC01 AC05 AC10 CA23 CA36 DA03 DA07

DA13 DB10

5C064 BA01 BB02 BC06 BC18 BC20 BD01 BD08 BD09

5J104 AA01 AA12 AA16 EA04 EA15 EA16 JA03 NA02 NA37 PA07